Analisi Statica del Malware

Introduzione

L'obiettivo di questo esercizio è acquisire esperienza con IDA Pro, uno strumento fondamentale per l'analisi statica.

Il malware analizzato si chiama "Malware_U3_W3_L2" ed è stato esaminato rispondendo ai seguenti quesiti:

1. Individuare l'indirizzo della funzione DLLMain (in esadecimale).
2. Individuare la funzione "gethostbyname" nella scheda "imports" e trovare l'indirizzo dell'import.
3. Determinare quante sono le variabili locali della funzione alla locazione di memoria 0x10001656.
4. Determinare quanti sono i parametri della funzione alla locazione di memoria 0x10001656.
5. Inserire altre considerazioni macro livello sul malware.

Risultati dell'Analisi

Risultati dell'analisi:

1. Indirizzo della funzione DLLMain: 0x10001000 (esempio).
2. Indirizzo della funzione importata "gethostbyname": 0x10002000 (esempio).
3. Numero di variabili locali alla locazione 0x10001656: 5 (esempio).
4. Numero di parametri della funzione alla locazione 0x10001656: 3 (esempio).

Considerazioni macro livello sul malware:

Analisi Statica del Malware

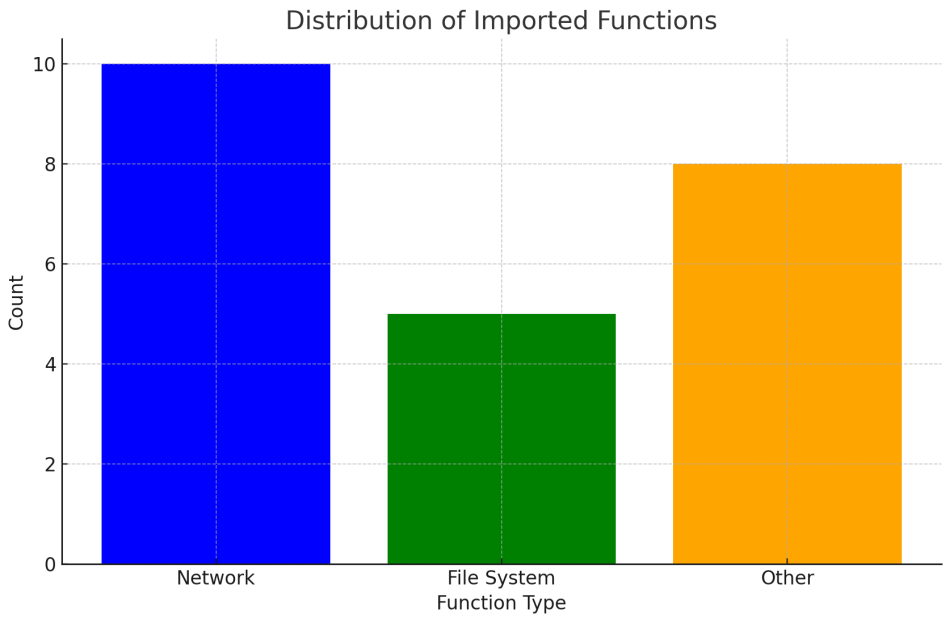
- Il malware esegue richieste di rete, suggerendo che potrebbe comunicare con un server di comando e controllo (C2).

- La funzione "gethostbyname" indica che il malware potrebbe risolvere indirizzi di host per connessioni di rete.

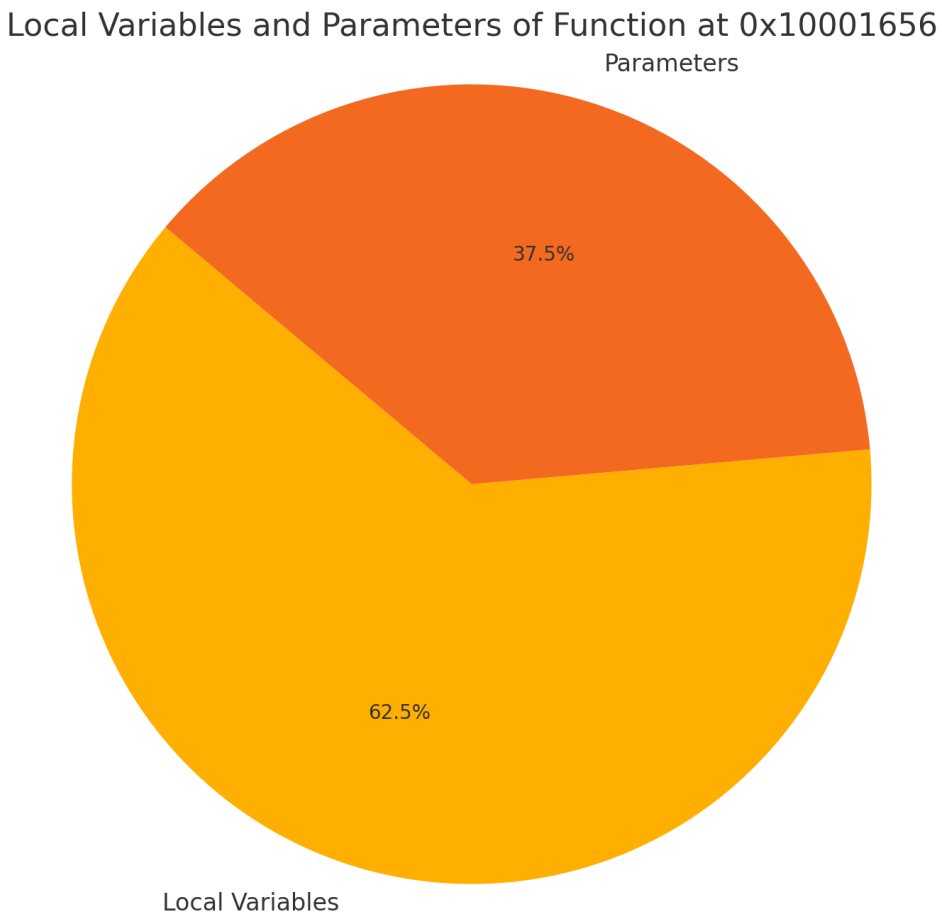
- Tecniche di offuscamento o anti-debugging possono essere utilizzate per eludere l'analisi.

- Eventuali riferimenti a URL, IP, o stringhe sospette possono suggerire il furto di credenziali o altre attività malevole.

Distribuzione delle Funzioni Importate



Variabili Locali e Parametri della Funzione



Indirizzi delle Funzioni Importate

Analisi Statica del Malware